What is Claimed:

1. A method of identifying the originator of a message transmitted between a client and a server system, said method comprising the steps of:

modifying a message to be transmitted during a session between a client and a server system to include a session identification flag and a session identifier corresponding to an originator of the session on the server system and allowing the originator of the session to be uniquely identified among originators of sessions on the server system;

transmitting the message between the client and the server system;

checking the transmitted message for the session identification flag; and

reading the session identifier of the transmitted message to determine the originator of the message.

2. The method according to claim 1, wherein the step of modifying the message comprises the step of re-computing a control portion of the message to reflect the inclusion of the session identification flag and the session identifier.

3. The method according to claim 2, further comprising the steps of:

removing the session identification flag and the session identifier from the transmitted message; and

re-computing the control portion of the message to reflect the removal of the session identification flag and the session identifier.

4. The method according to claim 1, wherein the step of modifying the message comprises appending the session identification flag and the session identifier at an end of the message.

5. The method according to claim 1, wherein the step of modifying the message further comprises at least one of changing the session identifier for each communication or changing the session identifier at a predetermined interval.

6. A method of identifying the originator of a communication packet transmitted between a client and a server in a client/server system, said method comprising the steps of:

appending a session identifier and a security tag to the communication packet, the session identifier uniquely identifying the client in the client/server system;

authenticating the session identifier using the security tag; and if the appended session identifier is authenticated, determining the originator of the transmitted communication packet based on the appended session identifier.

7. The method according to claim 6, further comprising the step of:

establishing a common security tag in the client and server, wherein the step of appending the session identifier includes appending the common security tag to the communication packet to be transmitted between the client and the server such that a presence of the common security tag in the transmitted communication packet indicates that the session identifier is authenticated.

8. The method according to claim 7, further comprising the steps of:

if the appended session identifier in the transmitted communication packet is authenticated, processing the transmitted communication packet according to predetermined rules for transmitted communication packets with authenticated session identifiers; and

if the appended session identifier in the transmitted communication packet is not authenticated, processing the transmitted communication packet according to predetermined rules for transmitted communication packets without authenticated session identifiers.

9. The method according to claim 8, wherein the step of appending the session identifier and the common security tag to the communication packet comprises the step of re-computing a control portion of the communication packet to be transmitted to reflect the inclusion of the common security tag and the session identifier, the method further comprising the steps of:

removing the common security tag and the session identifier from the transmitted communication packet; and

re-computing the control portion of the transmitted communication packet to reflect the removal of the common security tag and the session identifier.

10. The method according to claim 9, further comprising the steps of:

encrypting the communication packet to be transmitted after the step of appending the session identifier and the common security tag; and

decrypting the transmitted communication packet prior to the steps of determining the originator of the transmitted communication packet, removing the common security tag and the session identifier, and re-computing the control portion of the transmitted communication packet.

11. The method according to claim 9, further comprising the steps of:

encrypting the communication packet to be transmitted prior to the step of appending the session identifier and the common security tag; and

decrypting the transmitted communication packet after the step of re-computing the control portion of the transmitted communication packet.

12. The method according to claim 7, further comprising the step of:

setting a length of the common security tag greater than a predetermined length to reduce or substantially eliminate falsely authenticated session identifiers.

13. The method according to claim 12, wherein the length of the security tag is set to a length in the range of about 8 to 64 bits long.

14. A method of identifying an originator of all communication packets transmitted between a client and a server system using an application program, the originator having an actual network address, said method comprising the steps of:

modifying each of the communication packets to be transmitted between a client and a server system to include information identifying the originator of a respective communication packet without regard for the application program being used or an apparent network address that is a network address that replaces the actual network address of the originator during transmission of a respective communication packet;

transmitting each modified communication packet between the client and the server system; and

determining the originator of each transmitted communication packet based on the information identifying the originator therein.

15. A computer system for identifying the originator of a message, comprising:

a server; and

a client operationally connected to the server, the client and server being configured to transmit one or more messages therebetween during a session, each of the messages to be transmitted being modified by one of the client or the server to include a session identification flag and a session identifier, the client and server being further configured such that:

the modified message is transmitted to the remaining one of the client and the server;

the session identification flag of the transmitted message is checked by the remaining one of the client and the server to validate the session identifier; and

if the session identifier is validated, the session identifier of the transmitted message is read to determine the originator of the transmitted message, the session identifier corresponding to an originator of a session on the server system and allowing the originator of the session to be uniquely identified among originators of sessions on the server system.

16. The computer system according to claim 15, further comprising a network gateway disposed operationally between the client and server and providing access to the server such that the server is remotely accessible by the client.

17. The computer system according to claim 16, further comprising:

an encrypting unit disposed on one side of the network gateway to encrypt the message to be transmitted.

18. The computer system according to claim 17, further comprising:

a decrypting unit disposed on another side of the network gateway to decrypt the transmitted message.

19. The computer system according to claim 18, wherein the message is processed sequentially such that either the message to be transmitted is encrypted by the encrypting unit and then modified and the transmitted message is read and then decrypted by the decrypting unit or the message to be transmitted is modified and then encrypted by the encrypting unit and the transmitted message is decrypted by the decrypting unit and then read.

20. The computer system according to claim 16, wherein the network gateway includes a database to validate the session identifier by checking a user identifier, if the session identifier is not valid, the computer system forces the user to log in prior to accessing the server and if the session identifier is valid, the computer system retrieves an associated user identifier and the server processes the transmitted message.

21. A computer readable carrier including computer program instructions which cause a computer system including at least a client and a server to implement a method of identifying the originator of a message transmitted between the client and the server, said method comprising the steps of:

modifying a message to be transmitted during a session between the client and the server to include a session identification flag and a session identifier, the session identifier being assigned corresponding to the originator of the session on the server system and allowing the originator of the session to be uniquely identified among originators of sessions on the server system;

re-computing a control portion of the message to reflect the inclusion of the session identification flag and the session identifier;

transmitting the message between the client and the server;

checking the transmitted message for the session identification flag;

reading the session identifier of the transmitted message to determine the originator of the message;

removing the session identification flag and the session identifier from the transmitted message; and

re-computing the control portion of the message to reflect the removal of the session identification flag and the session identifier.